UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA
Plaintiff,

v. **Case No. 07-CR-171**

DAVID SZYMUSZKIEWICZ
Defendant.

DECISION AND ORDER

The government charged defendant David Szymuszkiewicz with three counts of interception of an electronic communication, contrary to 18 U.S.C. § 2511(1)(a). Defendant pleaded not guilty, and the case proceeded to trial. Defendant moved for entry of judgment of acquittal at the close of the government's case and again at the close of all evidence. See Fed. R. Crim. P. 29(a) ("After the government closes its evidence or after the close of all the evidence, the court on the defendant's motion must enter a judgment of acquittal of any offense for which the evidence is insufficient to sustain a conviction."). I reserved decision on both motions and submitted the case to the jury, which convicted on all counts. Defendant renewed the motion after discharge of the jury, and I granted the parties a chance to brief the issues. The matter is now fully briefed and ready for decision.

I. APPLICABLE LEGAL STANDARD

A defendant challenging the sufficiency of the evidence presented to the jury faces an "uphill battle," United States v. Gallardo, 497 F.3d 727, 737 (7th Cir. 2007), cert. denied, 129 S. Ct. (2008), one the Seventh Circuit has characterized as "nearly insurmountable," United States v. Knox, 540 F.3d 708, 719 (7th Cir. 2008), cert. denied, 129 S. Ct. 1525 (2009). In

ruling on a Rule 29 motion, the district court must view the evidence in the light most favorable to the government, bearing in mind that it is the exclusive function of the jury to determine the credibility of witnesses, resolve evidentiary conflicts and draw reasonable inferences. United States v. Reed, 875 F.2d 107, 111 (7th Cir. 1989). Because "Rule 29(c) does not authorize the judge to play thirteenth juror," the court may not entertain an independent view of the evidence in ruling on such a motion. United States v. Genova, 333 F.3d 750, 757 (7th Cir. 2003). Rather, it may enter a judgment of acquittal "only if, viewing the evidence in the light most favorable to the prosecution, the record contains no evidence on which a rational jury could have returned a guilty verdict." United States v. Murphy, 406 F.3d 857, 861 (7th Cir. 2005); see also United States v. Pulido, 69 F.3d 192, 205 (7th Cir. 1995) ("Reversal is warranted only when the record is devoid of any evidence, regardless of how it is weighed, from which a jury could find guilt beyond a reasonable doubt.") (internal quote marks omitted). If the court reserved ruling on a motion made during trial, it decides the motion based on the evidence at the time ruling was reserved. Charles A. Wright, Federal Practice and Procedure § 462, at 282 (2000).

II. DISCUSSION

In order to obtain a conviction in this case, the government had to prove (1) that defendant intercepted an electronic communication; and (2) that he did so intentionally. The term "intercept" means to acquire the contents of any electronic communication through the use of any electronic, mechanical or other device. An "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral or electronic communication. Finally, the term "intentionally" means to act deliberately and purposefully; that is, defendant's act had to be the product of his conscious objective rather than the product of

a mistake or an accident. (Jury Instructions at 16-17.) The government presented sufficient evidence for a reasonable jury to find these elements beyond a reasonable doubt.

A. The Government's Case

The government alleged that defendant, a revenue officer with the IRS, created a "rule" on his supervisor Nella Infusino's computer, which auto-forwarded to defendant all of Infusino's e-mails. The government presented testimony from Infusino and another IRS employee, Theresa Memmel, that on April 28, 2006, while Memmel was training Infusino on the use of "Outlook" – the e-mail program utilized by the IRS – the two came upon the rule on Ifusino's computer. Memmel and Infusino were shocked by the discovery and called the computer support department. Infusino testified that she did not create the rule or intend for defendant to receive her e-mails.[1] IRS computer specialist David Tietz testified he responded to Infusino's call and viewed the rule, which was active, on her computer. Tietz stated that he disabled the rule, then deleted it. Tietz further testified that defendant never advised him that he was receiving Infusino's messages, nor did he learn that from his co-workers in tech support.

William Taylor, an investigator with the Treasury Department's Inspector General's Office, testified that he looked into the matter after Infusino discovered the rule. Taylor reviewed data on the IRS's Outlook server, looking for e-mails auto-forwarded by rule, pursuant to which he recovered twenty-one e-mails forwarded from Ifusino to defendant. (Govt. Ex. 21-

[1]Infusino specifically testified that she did not intend to send the e-mails depicted in government exhibits 57, 81 and 113, which corresponded to the three counts in the indictment, to defendant, and that there would be no legitimate reason for defendant to receive the information contained therein. Exhibit 81, for example, pertained to performance evaluations for the revenue officers under Infusino's supervision.

42.) Taylor also checked defendant's computer hard drive, where he located 116 additional e-mails auto-forwarded from Infusino, all of which had been opened and some of which had been moved to different folders within defendant's Outlook program, including a "personal" folder defendant had apparently created. (Govt. Ex. 43-156.) Taylor testified that the only auto-forwarded e-mails he found on defendant's computer came from Infusino.

The government also presented evidence of defendant's motive to snoop on Infusino, and his opportunity to access her computer and create the rule. Infusino testified that she supervised defendant from 2001 to 2005 or 2006, during which time she managed several IRS offices in southeast Wisconsin. Infusino testified that she used a laptop computer, which she carried with her when she visited the officers under her supervision. Infusino never saw defendant access her computer (and she did not provide him with her password), but she stated that at times she left the computer unattended in the Racine office where defendant worked. Infusino further testified that in 2003 and 2004 issues with defendant's work performance arose, as described in government exhibit 147.

This evidence was sufficient for the jury to reasonably conclude that defendant intentionally intercepted Infusino's e-mails.[2] First, the government presented evidence that Infusino's computer contained a rule that automatically forwarded her e-mails to defendant, and no one else. Infusino denied creating or authorizing the rule, or wanting defendant to receive her e-mails. Second, the government demonstrated that defendant received Infusino's e-mails

[2]The government also presented testimony from IRS systems administrator Michael Heinich, who indicated that the IRS's Outlook exchange servers are located outside the State of Wisconsin. Thus, an e-mail sent by one Wisconsin IRS employee to another Wisconsin IRS employee travels out of state. Based on this testimony, the government established a sufficient connection to interstate commerce. See 25 U.S.C. § 2510(12).

and introduced 137 such communications. Investigator Taylor recovered some of the messages from the IRS server but many more from defendant's hard-drive – some of which had been placed in a specially created "personal" folder, others of which defendant had attempted to delete. Taylor further testified that he found no evidence of similar rules on defendant's computer. Third, the government presented evidence of defendant's motive and opportunity to access Infusino's computer and create the auto-forwarding rule. The evidence showed that a rule can be created in just a few minutes, and that Infusino left her computer unattended in defendant's presence for a sufficient period of time. While the government presented no direct evidence that defendant created the rule, the jury could draw reasonable inferences from the circumstantial evidence. See, e.g., United States v. Ranum, 96 F.3d 1020, 1026 (7th Cir. 1996) ("The defendant's fraudulent intent can reasonably be inferred from the facts set forth, which demonstrate that Ranum had an opportunity to deceive the Government as well as a motive for doing so."); United States v. Donovan, 24 F.3d 908, 913 (7th Cir. 1994) ("In evaluating the government's evidence, we expect jurors to draw on their experience as well as their common sense to draw reasonable inferences from the circumstantial evidence.").

As the Seventh Circuit explained in United States v. Briscoe:

> Although the jury's verdict may not rest solely on the piling of inference upon inference ..., [t]he view that the prosecution's case must answer all questions and remove all doubts . . . of course, is not the law because that would be impossible; the proof need only satisfy reasonable doubt. Indeed, [j]uries are allowed to draw upon their own experience in life as well as their common sense in reaching their verdict. . . . While [c]ommon sense is no substitute for evidence, . . . common sense should be used to evaluate what reasonably may be inferred from circumstantial evidence.

896 F.2d 1476, 1505-06 (7th Cir. 1990) (internal citations and quote marks omitted; alteration and emphasis in original); see also United States v. Rose, 12 F.3d 1414, 1417 (7th Cir. 1994)

(stating that "there is nothing novel about establishing a crime through the use of circumstantial evidence"). Under these standards, the government's evidence was sufficient in this case. Therefore, I deny defendant's motion made at the close of the government's case.

B. The Defense Case

The defense case does not compel a different result. Defendant first presented testimony from Karen Kammers, a fellow revenue officer, who testified that she knew defendant was receiving Infusino's e-mails. She stated that at one point defendant asked Infusino, in her presence, "Why am I getting all these e-mails?" However, the jury was not required to believe Kammers, a friend of defendant and member of his union board of directors. Rather, the jury could believe Infusino, who testified that she did not know defendant was receiving her e-mails until she and Memmel stumbled upon the rule. See Reed, 875 F.2d at 111 (stating that on Rule 29 review the court must bear in mind that it is the exclusive function of the jury to determine the credibility of witnesses).[3]

Defendant next called Doreen Greenwald, another revenue officer and union official. Greenwald also testified that defendant told her of his receipt of Infusino's e-mails, and she advised him that the fault would lie with the sender rather than the recipient. Again, the jury did not have to believe this testimony, and assessing witness credibility falls "within the jury's province." United States v. Hach, 162 F.3d 937, 942 (7th Cir. 1998).[4] Greenwald further testified that it was not uncommon at the IRS for a supervisor to forward her e-mails to a stand-

[3]The jury could also question whether the vague statement defendant allegedly made – "Why am I getting all these e-mails?" – was sufficient to alert Infusino to the situation.

[4]I also note that both Kammers and Greenwald denied knowing that defendant was receiving confidential information via Infusino's e-mails.

in during a leave, then forget to turn the auto-forward off on return to work. Again, the jury could credit Infusino's testimony that she did not follow this practice in general, nor did she ever create or direct creation of an auto-forward rule passing her e-mails on to defendant.

In his testimony, defendant denied that he took any action to intercept Infusino's e-mails, including accessing her computer or creating the rule at issue; in fact, he stated that prior to his indictment in this case he had never heard of such rules. Defendant further stated that he told Infusino he was getting her e-mails, showing her one, and she said she would contact the computer department. He stated that he also told co-workers about the situation. Again, the jury did not have to credit defendant's testimony on these issues; instead, the jury was authorized to believe Infusino.

Defendant also testified and presented evidence as to his solid work performance, but the jury could reasonably conclude that the performance issues which arose in 2003 and 2004 gave him a motive to snoop on his supervisor. Defendant further testified that he lacked the computer skills needed to create a rule, but the jury could reasonably have rejected such testimony in favor of that offered by Memmel – that defendant spoke with her about computers at a high level of sophistication. I may not under Rule 29 invade the jury's province and resolve disputed issues of credibility or draw my own inferences from the evidence.

Defendant next presented testimony from Peter Mulholland, a retired IRS automation coordinator. Mulholland testified that IRS laptops are password protected, and that they automatically disconnect if untouched for fifteen minutes, requiring the user to log-on again. However, the evidence showed that a rule could be created in less than fifteen minutes, and that one could simply touch a key or move the mouse in order to keep a computer from disconnecting. Therefore, Mulholland's testimony did not defeat the government's evidence

as to defendant's opportunity to access Infusino's computer and create the rule.

Mulholland also echoed Greenwald's testimony that it was common for managers to forward their e-mails to the acting manager while out of the office.[5] Mulholland testified that when this was done it was the responsibility of the manager to turn off the transfer upon return to work, but managers sometimes forgot to do so. However, as noted above, Infusino denied forwarding her e-mails; rather, she put an "out of the office" message on her account. She further testified that she did not know how to create an auto-forwarding rule and did not solicit anyone to create such a rule for her. The jury was entitled to believe her.

Finally, defendant called a computer expert, Steven Odenthal, who testified that he reviewed the e-mails forwarded from Infusino to defendant and observed that they occurred only during the first half of the year (January to June) in 2003, 2004 and 2006, which he found unusual. He indicated that deletion by the recipient could cause a gap, but he nevertheless found the pattern odd. Odenthal further testified that he observed no pattern in the content of those messages defendant ostensibly saved; most were innocuous. Odenthal also stated that given the volume of e-mail Infusino received, he expected to see more of her e-mails at the other end, i.e. defendant's. Finally, Odenthal testified that Infusino sometimes received e-mails auto-forwarded by rule, and defendant sometimes replied, and it seemed odd to him that Infusino would not notice the "auto-forwarded" text in the message. Nothing in Odenthal's testimony compels acquittal. The gaps he observed could, as he conceded, be caused by deletions. According to IRS policy, deleted messages remain on the server for fifteen days after which time they are gone forever. Further, Infusino testified that she lacked sophistication

[5]Defendant testified that he at times served as acting manager while Infusino was away.

in computer matters, so the fact that she did not detect the rule did not require the jury to reject her testimony. Therefore, I deny the motion made at the close of all evidence.

C. Defendant's Specific Challenges to the Sufficiency of the Evidence

In his post-trial briefs, defendant presents three specific challenges to the government's evidence. None require entry of a judgment of acquittal. Finally, defendant appeals to the rule of lenity, but because this case involves no serious statutory ambiguity that principle does not apply.

1. Use of a Device

Defendant first argues that the government failed to prove that he used a "device" to intercept Infusino's e-mails. The Wiretap Act provides that an "'electronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5). Relying on two district court cases addressing civil suits under the Wiretap Act, defendant argues that the statute requires use of a device separate and distinct from the drive and server upon which the communication was received. See Ideal Aerosmith, Inc. v. Acutronic USA, Inc., No. 07-1029, 2007 WL 4394447, at *4 (E.D. Pa. Dec. 13, 2007); Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001). These cases are distinguishable.

In Crowley, the plaintiffs electronically purchased items from Amazon.com, in the process transferring to Amazon certain personal information. Amazon, in turn, relayed some of this information to CyberSource for purposes of verifying the plaintiffs' credit. CyberSource then shared the information with others and used it to create purchaser profiles. Id. at 1267. The plaintiffs sued, alleging a violation of the Wiretap Act based on the events that began with

their electronic communications to Amazon. The court dismissed the claim, reasoning:

> Amazon did not, however, "intercept" the communication within the meaning of the Wiretap Act, because Amazon did not acquire it using a device other than the drive or server on which the e-mail was received. . . . Amazon merely received the information transferred to it by Crowley, an act without which there would be no transfer. Amazon acted as no more than the second party to a communication. This is not an interception as defined by the Wiretap Act.
>
> Crowley's argument, moreover, would result in an untenable result. Holding that Amazon, by receiving an e-mail, intercepted a communication within the meaning of the Wiretap Act would be akin to holding that one who picks up a telephone to receive a call has intercepted a communication and must seek safety in an exemption to the Wiretap Act. Such a result would effectively remove from the definition of intercept the requirement that the acquisition be through a "device." Therefore, the amended complaint fails to state a claim against Amazon under the Wiretap Act, and Amazon's motion to dismiss that claim is granted.

Id. at 1269.

In Ideal Aerosmith, Inc. v. Acutronic USA, Inc., the plaintiff, Ideal, attempted to acquire a bankrupt competitor, Carco, hiring Carco employees to continue operating the business and preserve its assets during the pendency of the bankruptcy proceedings. During this time, the former Carco employees continued to use their Carco e-mail addresses. Subsequently, the defendant, Acutronic, also a competitor, outbid Ideal and obtained Carco's assets. Thereafter, the ex-Carco employees hired by Ideal were assigned new, Ideal e-mail addresses. However, some ex-Carco employees and third parties doing business with Ideal inadvertently continued to send communications using the old Carco e-mail addresses. Plaintiff alleged that Acutronic, which now owned the Carco servers, caused the Carco servers to redirect those messages to an Acutronic server, thereby allowing Acutronic to read the messages. 2007 WL 4394447, at *2. Relying on Crowley, the court dismissed the claim, stating:

> In support of its wiretapping claims, Ideal has alleged that, after Acutronic purchased Carco, certain e-mail messages (the "Ideal Emails") were sent by Ideal's employees, including former Carco employees hired by Ideal, and by third

> parties conducting business with Ideal, to web addresses utilizing the Carco domain name. These e-mail messages were received by the Carco servers, now owned by Acutronic, and "redirected" by Acutronic to its own servers and/or forwarded to and among the other Defendants.
>
> These allegations do not state a claim of wiretapping. . . . Plaintiff has failed to allege the use of a device to intercept the communications. The drive or server on which an e-mail is received does not constitute a device for purposes of the Wiretap Act.
>
> . . .
>
> Here, there is no dispute that the Ideal E-mails were sent directly to Carco's server, now owned by Acutronic. Acutronic employed no device to acquire these e-mails, but was merely, as owner of Carco's system, a direct party to the communication. While Ideal complains that Acutronic was not the intended recipient of the communication, that argument has no legal bearing where the communication was nonetheless sent to Carco/Acutronic.

Id. at *4-5 (internal citations omitted).

In sum, Crowley and Ideal both concerned defendants who received information directed by the sender to them; in neither case did the defendants take any action to re-direct to themselves a communication addressed to another.[6] In other words, they were guilty only of passive receipt.

In the present case, conversely, the government did not rely solely on defendant's passive receipt of Infusino's e-mails on his own IRS computer via the IRS server. Rather, the government claimed that he used a device, i.e. Infusino's computer, to create the rule to intentionally effectuate re-direction/interception. He then used his own computer to receive and read the re-directed e-mails.

---

[6]It is true that the communications at issue in the Ideal case were intended for Ideal, not Acutronic/Carco. But as the court explained, the recipient of a misdirected e-mail is not guilty of interception. Id. at *5 n.2. Contrary to defendant's suggestion, the Ideal court did not address Acutronic's alleged forwarding of the e-mails from the Carco servers to Acutronic servers. Acutronic owned the Carco servers; thus, it was a direct party to the initial communication; what occurred later was irrelevant for purposes of the wiretap claim. See id. at *5.

This case would be like Crowley if Infusino had deliberately sent or forwarded an e-mail to defendant, then claimed a wiretap violation because he later shared the information with others in a manner she disapproved. This case would be like Ideal if Ifusino had mistakenly forwarded her e-mails to defendant, he read or forwarded them to others, and she then accused him of unlawful interception. As explained above, that is not what happened here; the government shouldered the burden of showing that defendant intentionally re-directed Infusino's e-mails to himself, not that he merely received them.

Defendant cites no case holding that use of two computers, as alleged by the government in this case, may not satisfy statutory requirements. Nor does he cite any case holding that use of some specialized equipment is required. The statutory definition of the term "device," set forth above, is broad enough to encompass this situation. Therefore, I reject this argument for acquittal.

2. Contemporaneous Interception

Second, defendant argues that the government failed to prove "contemporaneous" interception of the e-mails. He cites cases holding that a violation of the Wiretap Act requires interception of a communication simultaneous with its original transmission, rather than at some later point while the communication is "stored." See, e.g., Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002); Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 461-62 (5th Cir. 1994); Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 979-81 (M.D. Tenn. 2008). He states that in this case the e-mails sent to Infusino's computer were not intercepted by his computer contemporaneous to the original transmission; instead, after receipt Infusino's computer routed the e-mails back through the IRS server, which then forwarded them to defendant's computer.

These cases are distinguishable on their facts. In Konop, 302 F.3d at 878, the court found no violation of the Wiretap Act where the defendant gained access to the plaintiff's secure website and viewed bulletins posted there. In Cardinal Health, 582 F. Supp. 2d at 970-71, the court found no Wiretap Act violation where a former employee continued to log on to the employer's system using another employee's user-name and password, reading and reviewing the messages that the other employee received on his e-mail account. Finally, in Steve Jackson Games, Inc., 36 F.3d at 460, agents seized a computer on which was stored private e-mail that had been sent to an electronic bulletin board but not yet read by the recipients. In the present case, defendant did not access Infusino's messages on her computer after receipt. Rather, the messages destined for Infusino were auto-forwarded to defendant as soon as they were received on the IRS e-mail server. Further, as the government notes, the e-mails relating to the three counts of conviction reflect that they were sent to Infusino and defendant at the same time (accounting for a time zone difference). (Govt. Ex. 57, 81, 113.) With respect to Exhibit 57 in particular, Agent Taylor testified that the e-mail was submitted to the server at 2:23:58, a version created for defendant at 2:23:58, and the version so created delivered to defendant at 2:23:58. Thus, the government demonstrated contemporaneous interception.

In his reply brief, defendant cites a district court case which extended Konop and Steve Jackson Games even further. In Bunnell v. Motion Picture Ass'n of America, 567 F. Supp. 2d 1148 (C.D. Cal. 2007), the defendant hacked into the plaintiffs' e-mail system, then enabled the e-mail server software's "copy and forward" function, configuring it so that every incoming and outgoing email message would also be copied and forwarded to his e-mail account. Id. at 1150. The court held that, under Konop and its progeny, any communication acquired when

in storage, even if said storage lasted only momentarily on the server, fell outside the purview of the Wiretap Act. Id. at 1153-54. Defendant argues that, under Bunnell, even if he did access Infusino's computer and create the rule, he did not violate the Wiretap Act because the e-mails were accessed from the IRS server, not contemporaneously during their transmission from the senders.

In the sur-reply I permitted the government to file, the government attempts to distinguish Bunnell on its facts, arguing that in that case the messages were stored on the server, copied, then forwarded. In this case, the government says, messages sent to Infusino were as a matter of course routed through the IRS server, at which point they were simultaneously delivered to Infusino and defendant by operation of the rule. It is hard to see a meaningful difference, and the Bunnell holding appears to be a reasonable extension of the logic employed by Konop and Steve Jackson Games. The government's better response to Bunnell is legal – that court's extreme definition of "storage" makes it virtually impossible to prosecute the interception of e-mail under the Wiretap Act.

The Seventh Circuit has not spoken on this issue, but other circuits have questioned the general approach taken in the cases cited above, including Konop and Steve Jackson Games, and have by implication rejected the extension of this approach taken in Bunnell. In United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005) (en banc), the court discussed the manner in which e-mail is transmitted, traced the history of the relevant statutory provisions, and then held that the Wiretap Act applies to e-mail messages in the "transient electronic storage that is intrinsic to the communication process for such communications." See also Hall v. EarthLink Network, Inc., 396 F.3d 500, 503 n.1 (2d Cir. 2005) (rejecting the argument that "communication over the Internet can only be electronic communication while it is in transit,

not while it is in electronic storage"). I find that the Councilman approach makes more sense. To explain why, I first discuss the manner in which e-mails are transmitted across the internet, then apply the applicable statutory provisions.

The internet is a network of interconnected computers. After a user comprises and sends an e-mail, the message is broken down into small "packets," which are forwarded from one computer to another until they reach their destination, where they are reconstituted. Councilman, 418 F.3d at 69 (citing Orin S. Kerr, Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't, 97 Nw. U.L. Rev. 607, 613-14 (2003)). Each computer along the route stores the packets in memory, retrieves the addresses of their final destinations, and then determines where to send them next. At various points the packets are reassembled to form the original e-mail message, copied, and then re-packetized for the next leg of the journey. Once all the packets reach the recipient's mail server, they are reassembled to form the e-mail message. A mail delivery agent ("MDA") accepts the message, determines which user should receive the message, and performs the actual delivery by placing the message in that user's mailbox. Once the MDA has deposited an e-mail into the recipient's mailbox, the recipient must use an e-mail client program to retrieve and read the message. While this transmission process involves several steps, it usually takes just a few seconds, with each intermediate step taking well under a second. Id. at 69-70; see also Recent Development, A Thinly Veiled Request for Congressional Action on E-Mail Privacy: United States v. Councilman, 19 Harv. J.L. & Tech. 211, 216-17 (2005) (hereafter "Recent Development") (describing the manner in which e-mail is transmitted over the internet).

Congress first comprehensively addressed the issue of communications privacy in the 1968 Wiretap Act. The Act generally forbid the unauthorized, private interception of "wire

communications." See Recent Development, supra, at 213. Congress extended protection to e-mail and other electronic communications in the Electronic Communications Privacy Act ("ECPA") of 1986. The ECPA contains two relevant parts: the Wiretap Act and the Stored Communications Act ("SCA"). See id. at 214; see also Samantha L. Martin, Interpreting the Wiretap Act: Applying Ordinary Rules of "Transit" to the Internet Context, 28 Cardozo L. Rev. 441, 442 (2006); Michael D. Roundy, Reconcilable Differences: A Framework for Determining the "Interception" of Electronic Communications Following United States v. Councilman's Rejection of the Storage/Transit Dichotomy, 28 W. New Eng. L. Rev. 403, 413 (2006).

Generally speaking, the Wiretap Act is designed to prohibit the unauthorized, prospective interception of electronic communications. See Martin, supra, at 442-43. The SCA prohibits the unauthorized access of stored electronic communications, "generally a 'one-time event designed to copy past communications in storage.'" Id. at 443 (quoting Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1231 (2004)). While the distinction between access to communications in storage, to which the SCA applies, and the ongoing interception of communications in transmission, to which the Wiretap Act applies, may seem clear in theory, the mechanics of e-mail transmission discussed above have caused confusion. Determining which part of the ECPA applies is crucial, because the Wiretap Act prohibits private parties from ever intercepting communications and requires specific procedures be followed before law enforcement may do so. See id. at 443-44. I first examine the statutory language.

The Wiretap Act makes it a crime "to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). The term:

"electronic communication" means any transfer of signs, signals, writing, images,

> sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--
>
> (A) any wire or oral communication;
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
>
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds

18 U.S.C. § 2510(12). The statutory definition of "electronic communication" does not exclude messages in storage, and by its terms appears broad enough to include at least those communications stored temporarily as part of the e-mail transmission process. See Councilman, 418 F.3d at 72-73. Some courts have nevertheless concluded that communications in such storage should be excluded from the coverage of the Wiretap Act. They do so primarily in reliance on a different provision (since repealed) – the Act's definition of the term "wire communication."

In 1986, Congress added to the definition of "wire communication" the phrase "any electronic storage of such communication." Roundy, supra, at 414. Electronic storage is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). Some courts concluded, based on the absence of similar language in the definition of "electronic communication," that the Wiretap Act did not cover stored electronic communications. See, e.g., Steve Jackson Games, 36 F.3d at 461. Given the broad definition of stored communications, these courts further concluded that even

that temporary storage incidental to the transmission process took an e-mail outside the coverage of the Wiretap Act. See, e.g., id. at 461-62.

The statutory language does not support the inferential leap taken by these courts. As indicated above, the definition of "electronic communication" contains specific exclusions, but "electronic storage" is not one of them. This shows that "Congress knew how to, and in fact did, explicitly exclude four specific categories of communications from the broad definition of 'electronic communication.'" Councilman, 418 F.3d at 75. "Where Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent." Andrus v. Glover Constr. Co., 446 U.S. 608, 616-617 (1980). Of particular significance here is the statute's exclusion of "electronic funds transfer information stored by a financial institution." If Congress intended to exclude all stored electronic communications, this provision, excluding a narrow category of such communications, would be superfluous. See Roundy, supra, at 429-30. Statutes are to be construed to give effect to every clause, avoiding the creation of surplusage. See, e.g., TRW Inc. v. Andrews, 534 U.S. 19, 31 (2001).

Nor does the legislative history support the notion that communications in temporary electronic storage are outside the scope of the Wiretap Act. As the Councilman court explained, in enacting the ECPA Congress considered a study from the Congressional Office of Technology Assessment on the privacy implications of electronic surveillance. 418 F.3d at 76 (citing Office of Technology Assessment, Federal Government Information Technology: Electronic Surveillance and Civil Liberties (1985) ("OTA Report")).

> The report identified the different points at which an e-mail message could be intercepted:

> There are at least five discrete stages at which an electronic mail message could be intercepted and its contents divulged to an unintended receiver: at the terminal or in the electronic files of the sender, while being communicated, in the electronic mailbox of the receiver, when printed into hardcopy, and when retained in the files of the electronic mail company for administrative purposes. Existing law offers little protection.

Id. at 76 (quoting OTA Report at 48).

> Responding to concerns raised in the OTA Report, Congress sought to ensure that the messages and by-product files that are left behind after transmission, as well as messages stored in a user's mailbox, are protected from unauthorized access. E-mail messages in the sender's and recipient's computers could be accessed by electronically "breaking into" those computers and retrieving the files. OTA Report at 48-49. Before the ECPA, the victim of such an attack had few legal remedies for such an invasion. Furthermore, the e-mail messages retained on the service provider's computers after transmission – which, the report noted, are primarily retained for "billing purposes and as a convenience in case the customer loses the message" – could be accessed and possibly disclosed by the provider. Id. at 50. Before the ECPA, it was not clear whether the user had the right to challenge such a disclosure. Id. Similar concerns applied to temporary financial records and personal data retained after transmission. Id.
>
> Given this background and the evidence in the legislative history that Congress responded to the OTA Report in refining the legislation, see, e.g., House Hearings at 42-73, it appears that Congress had in mind these types of pre- and post-transmission "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," see 18 U.S.C. § 2510(17), when it established the definition of "electronic storage." Its aim was simply to protect such data. . . . There is no indication that it meant to exclude the type of storage used during transmission from the scope of the Wiretap Act.

Id. at 77-78.

The legislative history also reveals that the 1986 addition of the "storage" language to the definition of "wire communication" was intended, not to draw a distinction with "electronic communication," but to bring voice mail within the coverage of the Act. See id. at 78; Roundy, supra, at 414; 431. There is no suggestion in the history that this addition was intended to remove electronic communications from the coverage of the Wiretap Act during those periods

of storage incident to transmission. Councilman, 418 F.3d at 78. As one commentator has explained:

> Because wire communications can take place entirely absent any electronic storage, Congress wanted to indicate clearly that the wiretap law was also meant to cover the storage of such communications, such as in a voice mail system. In contrast, the technology underlying electronic communications makes it impossible for such transfers to occur without the use of electronic storage at various points along the transmission path. Thus, no explicit inclusion of electronic storage was needed in the definition of "electronic communication," since reading the text as excluding such intrinsic and inevitable storage would render the wiretap law's protection of electronic communications virtually meaningless.

Roundy, supra, at 431. This construction is bolstered by the fact that Congress removed the reference to electronic storage from the definition of wire communication (pursuant to the 2001 PATRIOT Act) in order to bring voice mail under the coverage of the more relaxed SCA, rather than the Wiretap Act. Councilman, 418 F.3d at 78-79 (citing Robert A. Pikowsky, An Overview of the Law of Electronic Surveillance Post September 11, 2001, 94 Law Libr. J. 601, 608 (2002)).

Finally, it would make little sense for Congress to decree that messages, which clearly constitute "electronic communications" under § 2510(12), briefly cease to be electronic communications for very short intervals while in "storage" en route to their final destination, then suddenly become electronic communications again. This result is all the more bizarre considering that this period of temporary "storage" is the point in time where it is technologically easiest to intercept those communications. Councilman, 418 F.3d at 78-79; see also Konop, 302 F.3d at 888 (Reinhardt, J., dissenting in part); Roundy, supra, at 404. Indeed, under the rationale of Steve Jackson Games and like cases, it is virtually impossible to "intercept" an e-mail under the Wiretap Act. See Konop, 302 F.3d at 888 (Reinhardt, J., dissenting in part);

Susan Freiwald, Online Surveillance: Remembering the Lessons of the Wiretap Act, 56 Ala. L. Rev. 9, 55, 83 (2004); Roundy, supra, at 426-28 & n.180; Jarrod J. White, E-Mail @ Work.Com: Employer Monitoring of Employee E-Mail, 48 Ala. L. Rev. 1079, 1083 (1997); see also Tatsuya Akamine, Proposal for a Fair Statutory Interpretation: E-Mail Stored in a Service Provider Computer is Subject to an Interception Under the Federal Wiretap Act, 7 J.L. & Pol'y 519, 526 (1999) (noting that commentators have criticized the consequences of Steve Jackson Games); Martin, supra, at 475-76 (discussing the possible use of a "sniffer" device to monitor e-mails in transient electronic storage).[7] Courts should not construe a statute so as it render it inconsequential. See Roundy, supra, at 426 (citing Haggar Co. v. Helvering, 308 U.S. 389, 394 (1940) ("A literal reading of [a statute] which would lead to absurd results is to be avoided . . . .")).[8]

Defendant argues that Councilman is distinguishable because the court there declined to address the contemporaneous interception argument he raises here. However, the

---

[7]As one commentator has explained, under Steve Jackson Games:

> there is only a narrow window during which an E-mail interception may occur – the seconds or mili-seconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of the ECPA is virtually impossible.

Jarrod J. White, E-Mail @ Work.Com: Employer Monitoring of Employee E-Mail, 48 Ala. L. Rev. 1079, 1083 (1997); see also Roundy, supra, at 403-04 (noting that under Steve Jackson Games and like cases, the simplest and cheapest forms of electronic interception would be allowed).

[8]Senator Leahy, the original sponsor of the ECPA, stated in an amicus brief in Councilman that the storage test is inconsistent with the legislative history and would render the Wiretap Act a dead letter as applied to e-mail. Roundy, supra, at n.198.

Councilman court avoided ruling on the issue only because the defendant's argument was based on the theory that "an e-mail in 'electronic storage' . . . cannot by definition be acquired 'contemporaneous with transmission.'" Id. at 80. Defendant makes largely the same argument here. In any event, to the extent that the term "intercept" carries with it a notion of contemporaneousness, for the reasons stated above, the government met its burden. The evidence showed that defendant intercepted Infusino's e-mails at the time of transmission, and via the rule he created did so in an ongoing, prospective fashion.

Commentators have noted that the Steve Jackson Games and Konop courts did not have to adopt a rigid storage/transit dichotomy to conclude that the conduct at issue in those cases was not covered by the Wiretap Act. See Roundy, supra, at 436; see also Recent Development, supra, at 222. Defining the term "intercept" to generally require contemporaneousness, see Konop, 302 F.3d at 878, would permit courts to maintain a distinction between prospective interception at the time of transmission and one-time access to information already received and in storage. See Roundy, supra, at 434-36. Such construction would avoid eliminating the protections of the Wiretap Act based on the transient storage incidental to e-mail communication.

To be clear, I have assumed that the term "intercept" in the Wiretap Act implies contemporaneousness. However, I reject the kind of rigid storage/transit distinction adopted by Bunnell, which renders virtually unenforceable the Act's protections for e-mails.

3. Intent

Third, defendant argues that the government failed to prove that he acted intentionally. He contends that the government offered only speculation and conjecture that he acted deliberately and purposefully in acquiring Infusino's e-mails. He notes that the government

presented no direct evidence as to how, when (and by whom) the rule on Infusino's computer was created; nor did the government rebut his testimony that he lacked the capacity to create such a rule, or present evidence that his computer contained such rules.

However, as discussed above, the prosecution's case need not answer all questions and remove all doubts, and a jury may convict based on circumstantial rather than direct evidence. For the reasons set forth in § II.A. of this decision, the government presented sufficient circumstantial evidence from which the jury could reasonably infer that defendant acted deliberately. As the government notes, the jury could in particular infer deliberateness based on the evidence that defendant not only opened the e-mails from Infusino but moved them to a "personal" items folder he created. The jury could also infer intent based on the fact that defendant apparently attempted to delete the e-mails by the time Agent Taylor searched his hard drive, and that Taylor found many of the e-mails in an off-line folder. See United States v. Hart, 273 F.3d 363, 373-74 (3d Cir. 2001) (holding that an attempt to conceal evidence raised an inference of the defendant's consciousness of guilt, and collecting cases); see also United States v. Miller, 159 F.3d 1106, 1110 (7th Cir. 1998) (holding that the jury could infer defendant's knowledge that property was stolen based on his attempt to conceal it). Further, the jury was entitled to disbelieve defendant's testimony that he never accessed Infusino's computer and that he lacked computer expertise, instead crediting the contrary testimony from Infusino and Memmel.

Defendant cites Wesley College v. Pitts, 974 F. Supp. 375, 381-82 (D. Del.1997) for the proposition that deliberate interception cannot be inferred from motive and unexplained receipt of another's e-mails. Noting the absence of any evidence of an affirmative step to access the e-mails, the Wesley College court entered summary judgment for the defendants. However,

unlike in Wesley College, where the plaintiff presented no evidence to support a conclusion that the defendant had the computer skills or the opportunity to infiltrate the e-mail system and acquire the e-mails, in the present case the government did present such evidence. As discussed above, the government presented evidence that defendant had access to Infusino's computer, and that he possessed the computer skill to create the rule.

4. Rule of Lenity

Finally, defendant appeals to the rule of lenity, but that "principle is only applicable where there is a grievous ambiguity or uncertainty in the language and structure of the Act." Ranum, 96 F.3d at 1030 (internal quote marks omitted). The definition of "device" in the Wiretap Act is sufficiently clear, and its application in this case creates no unfairness. Further, assuming that "contemporaneous interception" is required, the government presented sufficient evidence to so prove. Finally, this prosecution did not rest on the proposition that passive receipt of forwarded e-mails violates the Wiretap Act. The government shouldered the burden of proving that defendant engaged in an affirmative act, using a device other than his own computer upon which he received the e-mails, and that he received the e-mails simultaneous with their transmission. Therefore, the case presents no sharp departure from past practice, such that defendant did not receive fair notice of the (un)lawfulness of his conduct. See Councilman, 418 F.3d at 82-85 (rejecting similar arguments).

III. CONCLUSION

THEREFORE, IT IS ORDERED that defendant's motions for judgment of acquittal are **DENIED**.

IT IS FURTHER ORDERED that this matter is scheduled for **SENTENCING** on

Wednesday, September 9, 2009, at 1:30 p.m. The parties shall file any sentencing motions or memoranda no later than September 2, 2009.

FINALLY, IT IS ORDERED that defendant's June 22, 2009, request to travel in the entire state of Wisconsin and the Northern District of Illinois is **GRANTED**.

Dated at Milwaukee, Wisconsin, this 30th day of June, 2009.

/s Lynn Adelman

_____

LYNN ADELMAN
District Judge